

Claims

1. A method for validating a client device by a server device, said method comprising the steps of:

- generating a shared unpredictable secret;
- storing the shared unpredictable secret in the client device and in the server device;
- requiring the client device to prove that it holds a correct secret as a precondition to the server device validating the client device; and
- replacing the shared unpredictable secret by a new shared unpredictable secret when the server device validates the client device.

2. The method of claim 1 wherein an initial shared unpredictable secret is determined in the client device and in the server device during a registration step that occurs prior to a log-in step.

3. The method of claim 2 wherein the registration step entails more checking of bona fides of the client device than does a log-in step.

4. The method of claim 2 wherein, during the registration step, the client device is required to make a payment to the user device.

5. The method of claim 1 wherein the shared unpredictable secret is generated by a generator from the

1 group comprising a random number generator and a pseudo-random
2 number generator.

3
4 6. The method of claim 1 wherein the shared
5 unpredictable secret comprises an unpredictable component and
6 a fixed component.

7 7. The method of claim 1 wherein a plurality of client
8 devices desire to be validated by the server device; and
9 each client device has a unique unpredictable secret
10 that it shares with the server device.

11
12 8. The method of claim 1 wherein, following a validation
13 of the client device, the server device discards the original
14 shared unpredictable secret and stores within the server
15 device a new shared unpredictable secret that can be generated
16 by applying update data to the original shared unpredictable
17 secret.

18
19 9. The method of claim 1 wherein:
20 the server device sends update data to the client
21 device;
22 the client device applies the update data to the
23 shared unpredictable secret to generate a new
24 secret; and
25 the client device replaces the shared unpredictable
26 secret with the new secret.

27 10. The method of claim 9 wherein:
28

1 the server device generates the update data using a
2 generator from the group comprising a random
3 number generator and a pseudo-random number
4 generator; and

5
6 the step of applying the update data to the shared
7 unpredictable secret comprises computing a one-way
8 function of the combination of the shared
9 unpredictable secret and the update data.

10
11 11. The method of claim 9 wherein the client device
12 sends acknowledgement data to the server device to confirm
13 that the client device has replaced the shared unpredictable
14 secret with the new secret.

15 12. The method of claim 11 wherein, in response to the
16 server device receiving the acknowledgement data from the
17 client device, the server device:

18 validates the client device; and
19 discards the shared unpredictable secret and stores
20 within the server device the new secret, which now
21 becomes a new shared unpredictable secret.

22
23 13. The method of claim 11 wherein:
24 the client device sends to the server device proof
25 data demonstrating that the client device holds a
26 correct secret; and
27
28

1 the server device is adapted to accept from the
2 client device any proof data that are generated
3 from a secret that is newer than the secret for
4 which the most recent acknowledgment data have
5 been received by the server device.
6

7 14. The method of claim 11 wherein:

8 the client device sends to the server device both
9 the acknowledgment data and proof data derived
10 from the new secret.
11

12 15. The method of claim 14 wherein:

13 the proof data are computed on the new secret; and
14 the proof data serve also as acknowledgment data.

15 16. The method of claim 1 wherein:

16 the client device presents proof data to the server
17 device, wherein the proof data are derived from a
18 shared unpredictable secret using a proof data
19 generation algorithm, and the proof data do not
20 divulge the shared unpredictable secret;
21

22 the server device checks the proof data by using a
23 proof data generation algorithm consistent with
24 the proof data generation algorithm used by the
25 client device; and

26 when the server device determines that the proof
27 data presented by the client device were not
28

1 generated from the same shared unpredictable
2 secret that is stored in both the client device
3 and in the server device, the server device does
4 not validate the client device.
5

6 17. The method of claim 16 wherein each proof data
7 generation algorithm is a one-way function.
8

9 18. A system for enabling a server device to validate a
10 client device, said system comprising:

11 at least one client device;
12 a server device;
13 a shared unpredictable secret;
14 means for storing the shared unpredictable secret in
15 the client device;
16 means for storing the shared unpredictable secret in
17 the server device;
18 coupled to the client device and to the server
19 device, means for determining whether the client
20 device holds a correct secret;
21 coupled to the determining means, means for allowing
22 the server device to validate the client device
23 when the client device proves that it holds a
24 correct secret; and
25 coupled to the client device and to the server
26 device, means for replacing the original shared
27
28

1 unpredictable secret with a new shared
2
3 unpredictable secret when the server device
4 validates the client device.

5 19. A computer readable medium containing computer
6 program instructions for enabling a server device to validate
7 a client device, said computer program instructions causing
8 the execution of the following steps:

9 generating a shared unpredictable secret;
10 storing the shared unpredictable secret in the
11 client device and in the server device;
12 requiring the client device to prove that it holds a
13 correct secret as a precondition to allowing the
14 client device to be validated by the server
15 device; and
16 replacing the shared unpredictable secret by a new
17 shared unpredictable secret when the client device
18 is validated by the server device.
19
20
21
22
23
24
25
26
27
28